



# Integrating Active Directory with File Access Manager

Version: 8.4

Revised: March 27, 2023

---

## Copyright and Trademark Notices

### Copyright © 2023 SailPoint Technologies, Inc. All Rights Reserved.

All logos, text, content, including underlying HTML code, designs, and graphics used and/or depicted on these written materials or in this Internet website are protected under United States and international copyright and trademark laws and treaties, and may not be used or reproduced without the prior express written permission of SailPoint Technologies, Inc.

"SailPoint," "SailPoint & Design," "SailPoint Technologies & Design," "Identity Cube," "Identity IQ," "IdentityAI," "IdentityNow," "SailPoint Predictive Identity" and "SecurityIQ" are registered trademarks of SailPoint Technologies, Inc. None of the foregoing marks may be used without the prior express written permission of SailPoint Technologies, Inc. All other trademarks shown herein are owned by the respective companies or persons indicated.

SailPoint Technologies, Inc. makes no warranty of any kind with regard to this manual or the information included therein, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. SailPoint Technologies shall not be liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Patents Notice. <https://www.sailpoint.com/patents>

Restricted Rights Legend. All rights are reserved. No part of this document may be published, distributed, reproduced, publicly displayed, used to create derivative works, or translated to another language, without the prior written consent of SailPoint Technologies. The information contained in this document is subject to change without notice.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c)(1) and (c)(2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

Regulatory/Export Compliance. The export and re-export of this software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, licensee agrees to comply with all U.S. and foreign export laws and regulations as they relate to software and related documentation. Licensee will not export or re-export outside the United States software or documentation, whether directly or indirectly, to any Prohibited Party and will not cause, approve or otherwise intentionally facilitate others in so doing. A Prohibited Party includes: a party in a U.S. embargoed country or country the United States has named as a supporter of international terrorism; a party involved in proliferation; a party identified by the U.S. Government as a Denied Party; a party named on the U.S. Department of Commerce's Entity List in Supplement No. 4 to 15 C.F.R. § 744; a party prohibited from participation in export or re-export transactions by a U.S. Government General Order; a party listed by the U.S. Government's Office of Foreign Assets Control as ineligible to participate in transactions subject to U.S. jurisdiction; or any party that licensee knows or has reason to know has violated or plans to violate U.S. or foreign export laws or regulations. Licensee shall ensure that each of its software users complies with U.S. and foreign export laws and regulations as they relate to software and related documentation.

---

# Contents

---

- Active Directory Connector Overview** ..... **iv**
- Monitored Actions** ..... **v**
- Capabilities** ..... **6**
  - Supported Versions ..... 6
- Prerequisites** ..... **7**
  - Software Requirements ..... 7
  - Enabling the Audit Policy ..... 7
  - Active Directory User Permissions ..... 8
  - Communications Requirements ..... 8
- Active Directory Installation Flow Overview** ..... **9**
- Collecting Data Stored in an External Application** ..... **10**
  - Installation Locations ..... 11
- Adding an Active Directory Application** ..... **12**
  - Select Wizard Type ..... 12
  - General Details ..... 12
  - Connection Details ..... 13
  - Configuring and Scheduling the Permissions Collection ..... 14
  - Configuring Activity Monitoring ..... 22
  - Configuring Data Enrichment Connectors ..... 23
- Installing Services: Activity Monitor and Collectors** ..... **25**
- Verifying the Active Directory Connector Installation** ..... **28**
  - Installed Services ..... 28
  - Log Files ..... 28
  - Monitored Activities ..... 28
  - Permissions Collection ..... 28
- Special Configurations** ..... **30**
  - Excluding Domain Controllers Below Windows 2008 ..... 30
  - Monitoring Logon Events ..... 30

---

Excluding Objects from Monitoring .....	30
Crawling .....	31
<b>Troubleshooting .....</b>	<b>32</b>
Activities are not Shown in the Business Website .....	32
Errors in Accessing the Domain Controllers .....	32
No Events Found .....	32
Cannot Access Event Log .....	33

# Active Directory Connector Overview

## ***Activity Monitor***

File Access Manager Activity Monitor (Activity Monitor) for Active Directory (AD) is based on the native changes auditing capability in AD. AD writes these changes to the various domain controller event logs and the monitor collects them centrally so there is no need to install connectors on domain controllers.

The Activity Monitor service correlates the events and digests them, which makes events possible for people to read.

## ***GPO Auditing***

GPO auditing uses a proprietary method with no local connectors on the DCs. The method accesses all GPOs on all DCs through the SYSVOL share, and correlates GPO audit change events with the content of the GPOs.

## ***Domain Controllers***

To access the domain controllers, the Activity Monitor reads the list of all Domain Controllers from the domain every hour.

## ***Crawling***

Crawling and Permissions Collection work with standard LDAP queries to retrieve all the domain objects and analyze their respective permissions.

The Activity Monitor and Permissions Collector services can be installed on any server, including servers that are NOT members of the monitored domain. An application must be configured in File Access Manager for each monitored domain, with a separate set of Activity Monitor/Permissions Collection services, as described below.

## Monitored Actions

Action	Meaning
Create	An object was created in the domain.
Undelete	An object was restored in the domain.
Move	An object's location was changed in the domain.
Delete	An object was deleted in the domain.
FSMO Role Change	The owners of the domain FSMO roles were changed.
Audit Policy Change	The system audit policy was changed.
Domain Policy Change	The domain security policy was changed.
Account Lock	An account was locked, which includes the computer that originally caused the lock.
Account Logout	The account was logged out.
Reset Password	A user password was reset by another user.
Kerberos Pre-authentication failure	Kerberos pre-authentication failed.

Note 1: The old value will be empty and will not display in the Administrative Client if it was empty before the change. This is also true for the New value, if the attribute's value was deleted.

Note 2: The account logon is not monitored by default. (The Special Configuration section below describes how to configure the Activity Monitor to collect Account Logon events.)

## Capabilities

This connector enables you to use File Access Manager to access and analyze data stored in Active Directory and do the following:

- Analyze the structure of your stored data.
- Monitor user activity in the resources.
- Verify user permissions on the resources, and compare them against requirements.

See the File Access Manager documentation for a full description.

## Supported Versions

### *Activity Monitor*

The system supports auditing on domain controllers installed on Windows Server 2008 and above.

The relevant factor is the operating system of the domain controller. Not the domain functionality level.

### *Permissions Collection and Crawling*

Supported for all domain versions, forest versions, and operating systems.

## Prerequisites

Make sure your system fits the descriptions below before starting the installation.

## Software Requirements

File Access Manager requires the latest ASP.NET Core 6.0.x Hosting Bundle. This bundle consists of .NET Runtime and ASP .NET Core Runtime. You can download the latest 6.0.x Hosting Bundle version from [here](#).

## Enabling the Audit Policy

File Access Manager relies on the standard Active Directory advanced audit. The advanced audit overrides the simple audit, making the former obsolete. Be sure to migrate existing simple auditing to Advanced Auditing before proceeding.

This guide does not deal with complex GPO scenarios. Be sure that changes do not affect GPO precedence or corrupt other GPOs. Below is the settings in the Domain Controllers GPO.

Apply the following in a Domain Controller GPO.

1. Open “Default Domain Controller Policy”.
2. Navigate to *Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies*.
3. Set **Audit to success** in all the following settings:
  - *Account Management > Audit User Account Management*
  - *DS Access > Audit Directory Services Changes*
  - *Logon/Logoff > Audit Account Lockout*
  - *Policy Change > Audit Policy Change*
  - *Policy Change > Audit Authentication Policy Change*
  - *Policy Change > Audit Authorization Policy Change*

### **To enable login audits:**

Set Audit Kerberos Authentication Service to Success in Account Logon



## Active Directory User Permissions

The Active Directory user configured in the Application configuration below must be granted permissions to manage the audit settings of the domain objects, as well as to access the Domain Controller event logs.

1. Grant Manage Auditing and Security Log Privilege
  - a. Open Default Domain Controller Policy on a DC.
  - b.
    - Navigate to *Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment* and set the following settings:
      - Open *Manage auditing and security log* by double clicking or pressing **Enter**.
      - Add the domain user to the Users/Groups list.

The syntax of the user added to the list must be Domain\User.

2. Add the user to the “Event log readers” security group.

## Communications Requirements

Requirement	Source	Destination	Port
File Access Manager Message Broker	Permissions Collector	RabbitMQ	5671
File Access Manager server access	Activity Monitor/Permissions Collector	File Access Manager Servers	8000-8008
Event log remote	Activity Monitor	All Domain Controllers	MS RPC (135)
SYSVOL access	Activity Monitor	All Domain Controllers	CIFS/SMB (139, 445)
Additional queries	Activity Monitor/Permissions Collector	All Domain Controllers	LDAP (389)

The ‘Remote Event Log Management (RPC)’ inbound allow firewall rule must be enabled on the Active Directory (Domain Controller) servers.

## Active Directory Installation Flow Overview

To install the Active Directory connector:

1. Configure all the prerequisites.
2. Add a new Active Directory application in the Business Website.
3. Install the relevant services:
  - Activity Monitor - This is the activity collection engine, used by all connectors that support activity monitoring.
  - Permissions Collector

## Collecting Data Stored in an External Application

### Terminology:

#### **Connector**

The collection of features, components and capabilities that comprise File Access Manager support for an endpoint.

#### **Collector**

The “Agent” component or service in a Permission Collection architecture.

#### **Engine**

The core service counterpart of this architecture.

#### **Identity Collector**

A logical component used to fetch identities from an identity store and holds the configuration, settings for that identity store, and the relations between these identities.

The identity collector has no “physical” manifest.

- The actual work is done by the Collector Synchronizer.

The list below describes the high level installation process required to collect and analyze data from an external application. Most of these should already be set up in your File Access Manager installation. See the server Installation guide for further details.

#### **Install a Permission Collection central engine**

One or more central engines, installed using the server installer

#### **Create an Application in File Access Manager**

From the Business Website. The application is linked to central engines listed above.

#### **Add an Activity Monitor**

To collect activities for this application - run the Collector Installation Manager and add an application under Activity Monitoring.

### ***Install Permission Collectors (optional)***

Optionally, you can install collectors that will run on a separate server and take some of the work from the central PC and DC engines (Where supported). When installing a collector, you attach it to an engine. If no collectors are installed, the central services act as both the engine and the collector.

To install a collector, you must have the **RabbitMQ** service installed for communication between the central engines and the collectors. RabbitMQ is installed

For further details, see section **Application > Central Service > Collector Relations** in the File Access Manager Administrator Guide

## **Installation Locations**

### ***Activity Monitor***

Installed remotely on a File Access Manager monitor application server, which can be a server joined to any domain, including a domain different from the monitored domain.

## Adding an Active Directory Application

In order to integrate with Active Directory, we must first create an application entry in File Access Manager. This entry includes the identification, connection details, and other parameters necessary to create the link.

To add an application, use the **New Application Wizard**.

1. Navigate to *Admin > Applications*
2. Click **Add New** to open the wizard.

### Select Wizard Type

1. Click **Standard Application**
2. Click **Next** to open the **General Details** page.

### General Details

#### *Application Type*

Active Directory

#### *Application Name*

Logical name of the application

#### *Description*

Description of the application

#### *Tags*

Select tags for the application from the dropdown menu, and / or type a new name, and press **Enter** to create a new tag. The dropdown list of tags filters out matching tags as you type and displays up to 50 tags.

The **tags** replace the **Logical container** field that was used when creating applications in releases before 8.2

#### *Event Manager Server*

This option is available if there are more than one event manager servers configured in the system.

Select an event manager from the drop down menu.

## ***Identity Collector***

Select from the Identity Collector dropdown menu.

- You can create identity collectors in the administrative client. **Applications > Configuration > Permissions Management > Identity Collectors.**

See section "OOTB Identity Collection" in the Collector Installation Manager File Access Manager Administrator Guide for further details.

- If adding a new identity collector, press the **Refresh** button to update the Identity Collector dropdown list.

Click **Next.** to open the Connection Details page.

## **Connection Details**

### ***Domain Name***

FQDN of the domain.

### ***SSL***

Must be checked to connect with LDAPS.

### ***Domain NetBIOS Name***

The short name of the domain.

### ***Base DN***

Distinguished Name (DN) – The level in the AD tree from which to perform a search. This field should remain empty unless needed.

### ***Username***

The samAccountName of the user defined in the prerequisites, or the UPN if the user is from a different trusted domain.

### ***Password***

The user's password

If the user is from a different trusted domain, type the UPN in the User field (username@fqdn), and type the short name of the domain in the Domain NetBIOS Name.

### ***Specific Server Connection***

Connection through a specific server instead of selecting a DC dynamically

### ***Pool Size***

Number of parallel LDAP connections to DCs (Default is set to 50).

### ***Timeout***

Timeout for each LDAP query in seconds (Default is set to 15 sec).

Click **Next**.

## **Configuring and Scheduling the Permissions Collection**


Permissions can be analyzed to determine the application permissions of an out-of-the-box application, provided you have defined an identity store for File Access Manager to use in its analysis, and you have run a crawl for the application.

The permission collector is a software component responsible for analyzing the permissions in an application.

The Central Permission Collector Service is responsible for running the Permission Collector and Crawler tasks.

If the “FAM Central Permission Collector” wasn’t installed during the installation of the server, this configuration setting will be disabled.

### **To configure the Permission Collection**

- Open the edit screen of the required application.
  - a. Navigate to **Admin > Applications**.
  - b. Scroll through the list, or use the filter to find the application.
  - c. Click the edit icon  on the line of the application.
- Press **Next** till you reach the **Crawler & Permissions Collection** settings page.

The actual entry fields vary according to the application type.

When entering this page in edit mode, you can navigate between the various configuration windows using the **Next** and **Back** buttons.

### ***Central Permissions Collection Service***

Select a central permission collection service from the dropdown list. You can create permissions collection services as part of the service installation process. See section "Services Configuration" in the File Access Manager Administrator Guide for further details.

### ***Calculate Effective Permissions***

Calculate effective permissions during the permissions collection run.

### ***Calculate Riskiest Permissions***

Calculates the riskiest permission on a resource – for example, Full Control is riskier than Read permissions if both are on a resource.

This option is available when selecting **Calculate Effective Permissions**

### ***Skip Identities Sync during Permission Collection***

Skip identity synchronization before running permission collection tasks when the identity collector is common to different connector.

This option is checked by default.

## **Scheduling a Task**

### ***Create a Schedule***

Click on this option to view the schedule setting parameters.

### ***Schedule Task Name***

A name for this scheduling task

When creating a new schedule, the system generates a default name in the following format:

{appName} - {type} Scheduler

You can override or keep this name suggestion.

### ***Schedule***

Select a scheduling frequency from the dropdown menu.



- ***Schedule Types and Intervals***

***Once***

Single execution task runs.

***Run After***

Create dependency of tasks. The task starts running only upon successful completion of the first task.

***Hourly***

Set the start time.

***Daily***

Set the start date and time.

***Weekly***

Set the day(s) of the week on which to run.

***Monthly***

The start date defines the day of the month on which to run a task.

***Quarterly***

A monthly schedule with an interval of 3 months.

***Half Yearly***

A monthly schedule with an interval of 6 months.

***Yearly***

A monthly schedule with an interval of 12 months.

***Date and time fields***

Fill in the scheduling times. These fields differ, depending upon the scheduling frequency selected.


***Active check box***

Check this to activate the schedule.

Click **Next**.

## Configuring and Scheduling the Crawler

### *To set or edit the Crawler configuration and scheduling*

- Open the edit screen of the required application.
  - a. Navigate to **Admin > Applications**.
  - b. Scroll through the list, or use the filter to find the application.
  - c. Click the edit icon  on the line of the application.
- Press **Next** till you reach the **Crawler & Permissions Collection** settings page.

The actual entry fields vary according to the application type.

### **Create a Schedule**

Click to open the schedule panel.

### **Setting the Crawl Scope**

Note: When the crawl is performed, two resources will display but neither are added by the crawl. These two resources also cannot be removed from the scope.

**Configuration Resource:** for all activities that occur in the Configuration schema of the domain, which is shared across the forest. This means that in a multi-domain forest, you will still see it under the forest node rather than under the domain node.


**\_Audit Policy:** specifically for changes to the domain's audit policy, which are not really associated with any part of the domain tree, thus are given their own resource.

There are several options to set the crawl scope:

- Setting explicit list of resources to include and / or exclude from the scan.
- Creating a regex to define resources to exclude.

### **Including and Excluding Paths by List**

### ***To set the paths to include or exclude in the crawl process for an application***

- Open the edit screen of the required application.
  - a. Navigate to **Admin > Applications**.
  - b. Scroll through the list, or use the filter to find the application.
  - c. Click the edit icon  on the line of the application.
- Press **Next** till you reach the **Crawler & Permissions Collection** settings page.


The actual entry fields vary according to the application type.

  1. Scroll down to the Crawl configuration settings.
  2. Click **Advanced Crawl Scope Configuration** to open the scope configuration panel.
  3. Click Include / Exclude Resources to open the input fields.
  4. To add a resource to a list, type in the full path to include / exclude in the top field and click **+** to add it to the list.
  5. To remove a resource from a list, find the resource from the list, and click the x icon on the resource row.

When creating exclusion lists, excludes take precedence over includes.

### **Excluding Paths by Regex**

#### ***To set filters of paths to exclude in the crawl process for an application using regex.***

- Open the edit screen of the required application.
  - a. Navigate to **Admin > Applications**.
  - b. Scroll through the list, or use the filter to find the application.
  - c. Click the edit icon  on the line of the application.
- Press **Next** till you reach the **Crawler & Permissions Collection** settings page.

The actual entry fields vary according to the application type.

1. Click **Exclude Paths by Regex** to open the configuration panel.
2. Type in the paths to exclude by Regex, See regex examples in the section below. Since the system does not collect BRs that match this Regex, it also does not analyze them for permissions.

### Crawler Regex Exclusion Example

The following are examples of crawler Regex exclusions:

#### **Exclude all users (CNs) under specific department (OU):**

Example: All under Finance OU

Regex: `^CN=.,OU=finance,DC=office,DC=mydomain,DC=com$`

Example: All under Finance and Accounting OU

Regex: `^CN=.,OU=(finance|accounting),DC=office,DC=mydomain,DC=com$`

#### **Include ONLY users (CNs) under specific department (OU):**

Example: Only under Finance OU

Regex: `^(?! CN=.,OU=finance,DC=office,DC=mydomain,DC=com) $`

#### **Narrow down the selection:**

Include ONLY the C\$ drive shares: `\\server_name\C$`

Regex: `^(?!\\\\server_name\\C\$(\$|\\.*)) .*`

Include ONLY one folder under a share: `\\server\share\folderA`

Regex: `^(?!\\\\server_name\\share\$(\$|\\folderA$|\\folderA\\.*)) .*`

Include ONLY all administrative shares

Regex: `^(?!\\\\server_name\\[a-zA-Z]\$(\$|)).*`

To write a backslash or a Dollar sign, add a backslash before it as an escape character.

To add a condition in a single command, use a pipe character “|” .

### Excluding Top Level Resources

Use the top level exclusion screen to select top level roots to exclude from the crawl. This setting is done per application.

### ***To exclude top level resources from the crawl process***

1. Open the application screen

*Admin > Applications*

2. Find the application to configure and click the drop down menu on the application line. Select **Exclude Top Level Resources** to open the configuration panel.

3. ***Run Task***

The Run Task button triggers a task that runs a short detection scan to detect the current top level resources.

Before running the task for the first time, the message above this button is:

**"Note: Run task to detect the top-level resources"**

If the top level resource list has changed in the application while you are on this screen, press this button to retrieve the updated structure.

Once triggered, you can see the task status in

*Settings > Task Management > Tasks*

This will only work if the user has access to the task page

When the task has completed, press **Refresh** to update the page with the list of top level resources.

4. Click the top level resource list, and select top level resources to exclude.
5. Click *Save* to save the change.
6. To refresh the list of top level resources, run the task again. Running the task will not clear the list of top level resources to exclude.

## Top Level Resources Exclusion

WFS-DC testing

**Last Successful Run** 06-22-2021 4:57:27 PM

[Run Task](#) [View Task Status](#)

**Note:** Refresh the list to view recently discovered resources [Refresh](#)

**Top Level Resources Exclusion List** 0 Selected | [Clear Selection](#)

Top Level Resources Exclusion List

- \\si-...-5\C\$
- \\si-...-5\MSSQLSERVER
- \\si-...-5\print\$

### Special Consideration for Long File Paths in Crawl

If you need to support long file paths above 4,000 characters for the crawl, set the flag

**`excludeVeryLongResourcePaths`**

in the Permission Collection Engine App.config file to true.

By default this value will be commented out and set to false.

This key ensures, when enabled, that paths longer than 4000 characters are excluded from the applications' resource discovery (Crawl), to avoid issues while storing them in the SQLServer database.

When enabled, business resources with full paths longer than 4000 characters, and everything included in the hierarchical structure below them, will be excluded from the crawl, and will not be collected by File Access Manager. This scenario is extremely rare.

You should not enable exclusion of long paths, unless you experience an issue.

### Background

File Access Manager uses a hashing mechanism to create a unique identifier for each business resource stored in the File Access Manager database. The hashing mechanism in SQLServer versions 2014 and earlier, is unable to process (hash) values with 4,000 or more characters.

Though resources with paths of 4000 characters or longer are extremely rare, File Access Manager is designed to handle that limitation.

### ***Identifying the Problem***

When using an SQL Server database version 2014 and earlier

The following error message in the Permission Collection Engine log file:

```
System.Data.SqlClient.SqlException (0x80131904): String or binary data would be truncated.
```

In all other cases, this feature should not be enabled.

### ***Setting the Long Resource Path Key***


The Permission Collection Engine App.config file is `RoleAnalyticsServiceHost.exe.config`, and can be found in the folder

`%SailPoint_Home%\FileAccessManager\[Permission Collection instance]\`

Search for the key **`excludeVeryLongResourcePaths`** and correct it as described above.

## **Configuring Activity Monitoring**

### ***To configure the activity monitoring polling parameters***

- Open the edit screen of the required application
  - a. Navigate to **Admin > Applications**
  - b. Scroll through the list, or use the filter to find the application
  - c. Click the edit icon  on the line of the application
- Press **Next** till you reach the **Activity Configurations & Decs** settings page.

### ***Polling Interval (sec)***

Activity fetching interval [in seconds]. Default is set to 60 seconds,

### ***Report Interval (sec)***

Activity Monitor Health reporting interval [in seconds]. Default is set to 60 seconds.

### ***Local Buffer Size (MB)***

Local buffer size for activities [in MB]. Default is set to 200MB.

This cyclic buffer is used to store activities on the Application Monitor's machine in case of network errors that prevent the activities from being sent.

### Activity Data Retention Period

By default, this feature is disabled.

When selecting the Clear Activity Data option, a user is able to provide a time frame (1 to 100) in either months or years for all activity to be retained. Once that time period is met, all data will be removed.

A user can also select to backup the data before it is deleted by selecting the Backup Events Before Clearing option.

The Backup Before Clearing Option will only be enabled if the backup option is set during the system installation. If a user has not selected the backup option during the installation nor provided a backup path, this option will not be enabled.

The screenshot shows a configuration window titled "Activity Data Retention Period". Below the title is a descriptive sentence: "Activity data will be retained for the specified period. Following that time period, activities will be cleared." The main configuration area contains three elements: a checked toggle switch for "Clear Activity Data", a label "How long do you want to keep activity data? \*" followed by a numeric input field containing "12" and a unit dropdown menu set to "Month(s)", and another checked toggle switch for "Backup Events Before Clearing".

## Configuring Data Enrichment Connectors

The Data Enrichment Connectors (DEC) configuration enables us to select data enrichment sources. These can be used to add information from other sources about identities.

An enrichment source could be a local HR database that is used to combine users' job descriptions or departments to the information stored in the identity store.

Select the data enrichment connectors to enrich monitored activities from the Available DECs text box.

Use the > or >> arrows to move the selected DECs to the Current DECs text box.

The user can select multiple DECs. Simply select each desired DEC.



You can create a new DEC in the Administrative Client (Applications>Configuration>ActivityMonitoring>DataEnrichmentConnectors).

After creating a new DEC, click **Refresh** to refresh the dropdown list.

The chapter Connectors of the File Access Manager Administrator Guide provides more information on Data Enrichment Connectors, including what they are, how to configure them, and how they fit in the Activity Flow.

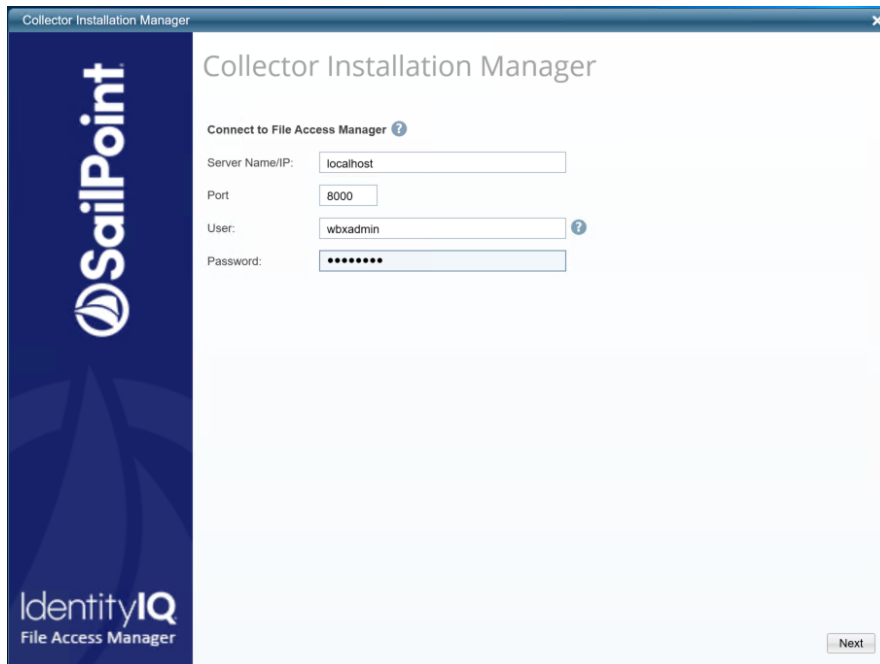
## Installing Services: Activity Monitor and Collectors

The Collector Installation Manager is part of the File Access Manager installation package. This tool is used to install the activity monitor, permission collector, and data classification collector.

1. Run the **Collector Installation Manager** as an Administrator.

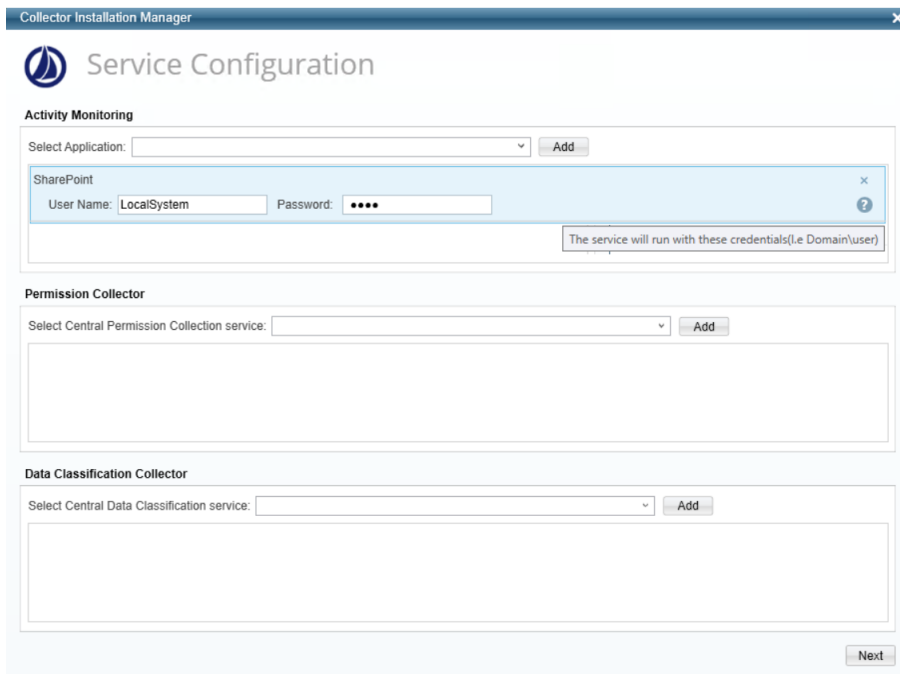
The installation files are in the installation package under the folder Collectors.

The Collector Installation Manager window displays.



2. Enter the credentials to connect to File Access Manager.
  - a. ServerName/IP should be pointed to the Agent Configuration Manager service server.
  - b. An File Access Manager user with Collector Manager permission (permission to install collectors). For Active Directory authentication, use the format domain\username.
3. Click Next.

The Service Configuration window displays.



4. If you are installing the Activity Monitor, select the application, and click **Add**.
5. When installing a SharePoint Activity Monitor, you will be prompted for service account credentials. This service account will be used by the Activity Monitor service to run the service and authenticate against the SharePoint IIS servers to fetch the logs (“Log on as”). Make sure the service account provided has local administrator privileges on the local server (hosting the Activity Monitor service) and can access the activity logs on the IIS servers.
6. If you are installing the Permission Collector, select the Central Permission Collector to which to connect this service, and click **Add**.
7. Click **Next**.

The Installation Folder window displays.

If this is the first time you are installing collectors on this machine, you will be prompted to select an installation folder, in which all future collectors will also be installed.

8. Browse and select the location of the target folder for installation.
9. Browse and select the location of the folder for system logs.
10. Click **Next**.

11. The system begins installing the selected components.
12. Click **Finish**.

The Finish button is displayed after all the selected components have been installed.

The File Access Manager Administrator Guide provides more information on the collector services.

## Verifying the Active Directory Connector Installation

### Installed Services

Verify that the services installed for the connector are available and active. Using windows Service manager, or other tool, look for the File Access Manager services, and see that they are running.

for example:

- File Access Manager Central Activity Monitor - <Application\_Name> service is running.
- File Access Manager Central Permissions Collection - <Application\_Name> service is running.

### Log Files

Check the log files listed below for errors

- "%SAILPOINT\_HOME\_LOGS%\PermissionCollection\_<Service\_Name>.log"
- "%SAILPOINT\_HOME\_LOGS%\ACTIVE DIRECTORY-<Application\_Name>.log"

### Monitored Activities

1. Simulate activities on Active Directory.
2. Wait a minute (approximately).
3. Verify that the activities display in the File Access Manager website under  
*Forensics > Activities*

### Permissions Collection

1. Run the Crawler and Permissions Collector tasks (*Settings > Task Management > Scheduled Tasks*)

2. Verify that:

- The tasks completed successfully
- Business resources were created in the resource explorer (*Admin > Applications > [application column] > Manage Resources*)
- Permissions display in the Permission Forensics page (*Forensics > Permissions*)

## Special Configurations

The following are a couple of configurations that may be needed:

### Excluding Domain Controllers Below Windows 2008

If there are domain controllers installed on an operating system older than Windows 2008, the system displays an error message in the Activity Monitor log, indicating that the Activity Monitor cannot connect to the Domain Controllers.

To exclude these Domain Controllers, perform the following steps:

1. Open the Activity Monitor service installation folder.
2. Edit the bamframework.exe.config.
3. Under <appSettings>, locate the key called "ExcludedDCs":<add key="ExcludedDCs" value="" />
4. Add the FQDN of the domain controllers to be excluded, separated by the |character:
5. <add key="ExcludedDCs" value="old-dc1.deprecated.com|old-dc2.10.years.old.os.com" />
6. Restart the Activity Monitoring service.

### Monitoring Logon Events

To add monitoring of Logon events, perform the following steps:

1. Open the Activity Monitor service installation folder.
2. Edit the bamframework.exe.config.
3. Under <appSettings>, locate the key called "readLogonEvents", and set it to true:  
<add key="readLogonEvents" value="true" />
4. Restart the Activity Monitor service.

### Excluding Objects from Monitoring

By default, SecurityIQ Activity Monitor excludes the dnsNode and msExchActiveSyncDevice object classes from monitoring.

To exclude additional object classes from monitoring, perform the following steps:

1. Open the Activity Monitor service installation folder.
2. Edit the bamframework.exe.config.
3. Under <appSettings>, locate the key called “excludedObjectClasses”, and set its value to the object classes to exclude:

```
<add key="excludedObjectClasses" value="dnsNode|msExchActiveSyncDevice"/>
```

The value must contain a list of object classes separated by the '|' character.

## Crawling

By default, SecurityIQ crawls and creates business resources for the following object types in the domain:

- User
- Group
- Organizational Unit (OU)
- Domain
- Computer
- Container

Overriding the default object types is not recommended, since they are the most common, and serve to exclude irrelevant object types (such as DNS records or Exchange Active Sync objects).

To override the default behavior, perform the following steps:

1. Open the Permissions Collector configured for the Active Directory Application installation folder.
2. Edit the RoleAnalyticsServiceHost.exe.config file.
3. Under the <appSettings> section, add the following key:

```
<add key="relevantTypes" value="objectClass|objectClass|...|objectClass" />
```

The value must contain a list of object classes separated by the | character and the domain object class must be one of the object classes in the defined list.

4. Restart the Permissions Collector service.



## Troubleshooting

Check the issues below for common problems and suggested ways of handling them.

### Activities are not Shown in the Business Website

- Verify that all prerequisites were set.
- Check the Activity Monitor logs for errors.

### Errors in Accessing the Domain Controllers

If there are errors in accessing the domain controllers, such as RPC server or server not available:

- Verify that this domain controller is running on Windows 2008 or above.
- Open the event viewer of the domain controller on which the change was made, with the user configured in the Application configuration.

If the viewer fails to open, verify that the user has the permissions described in the prerequisites section.

- Search for events with IDs 5136-5141.  
Verify the connection to the domain controller in which the change was made, and verify that the change audit policy was enabled as written in the prerequisites section.

### No Events Found

- Run the following command on the domain controller:

```
Auditpol /get /subcategory: "directory service changes"
```

- Verify that the settings described in [Enabling the Audit Policy](#) section are "Success".
  - If these settings are not defined, trigger a GPO update by running the following command:

```
gpupdate /force
```

- If the settings are still not defined, verify that the GPO is properly configured in, and applied to, the domain controller.

## Cannot Access Event Log

### *Event Viewer of the domain controller fails to open*

Open the event viewer of the domain controller on which the change was made, with the user configured in the Application configuration.

If the viewer fails to open, verify that the user has the permissions described in [Active Directory User Permissions](#).

### *Access is Denied(5) Error when trying to access Directory Services*

Navigate to *Event Viewer (DC server name) > Applications and services Logs > Directory Services* and verify that you have access to it.

If you get an **Access is Denied(5)** error (See image) , contact your Active Directory owner and ask to remove this restriction for the relevant SecurityIQ user. The access to Directory Service should be granted with EventLogReader group association.

